



401 – MSN SESSION LOGS AND CHAT

TEAM INFORMATION

Team Name:

AWGN

Results Email:

[REDACTED]

Examination Time Frame:

10/27/08

to

10/27/08

INSTRUCTIONS

Description: Examiners must develop and document a methodology used to parse MSN Session Logs and Chat communications from the presented MSN Chat program files contained in the folder **401_MSN_Session_Logs_and_Chat_Challenge2008** to an easily understandable and readable format. The supplied files were from either or both of the two computers used in the chat conversation. A detailed explanation of your process (software or technique) used to examine, extract, and present the data is required. A detailed explanation of your process (software or technique) used to examine, extract, and present the data is required.

Points will be awarded for the completeness of the data recovered from the communications and the ease of understanding or utility of the method the information is reported from that file(s).

Total Weighted Points: 80 Total Points available per entry – Total 400 Points Available

1. **Answers** – Fill in the chart below with your findings. *As a Forensic Challenge, consider that your answers will have to have enough detail for the Findings and Methodology of your examination to satisfy questioning in a court of law.*
2. **Methodology** – Provide a meticulously detailed explanation of your process. Be sure to include a step action that our reviewers can follow to reproduce your work for authenticity including tools and techniques.

INTERNAL REVIEWER USE ONLY

Reviewer:

Points Awarded:

Date:

Review Period:

to

Completed: ☐ Yes

☐ No

☐ Partial

Team AWGN 401

Page 1 of 6 11/18/2008

Challenge Number: 401 - MSN Session Logs and Chat

Examiner: Jeremy Roseboom



udorntani1744684863.xml

Date Time From To Message

4/3/2008 11:53:16 AM Zeus blane hey man whats up long time no talk
 4/3/2008 11:53:40 AM blane Zeus what are you talking about
 4/3/2008 11:53:52 AM Zeus blane just what i said
 4/3/2008 11:54:22 AM blane Zeus come on bob, quit horsing around, i know it's you.
 4/3/2008 11:54:29 AM Zeus blane ok, got me
 4/3/2008 11:54:39 AM Zeus blane just wanted to see if you'd bite
 4/3/2008 11:55:07 AM Zeus blane i switching back to normal sign on now

yogibear19534226628795.xml

Date Time From To Message

4/3/2008 11:53:16 AM Zeus blane hey man whats up long time no talk
 4/3/2008 11:53:40 AM blane Zeus what are you talking about
 4/3/2008 11:53:52 AM Zeus blane just what i said
 4/3/2008 11:54:22 AM blane Zeus come on bob, quit horsing around, i know it's you.
 4/3/2008 11:54:29 AM Zeus blane ok, got me
 4/3/2008 11:54:39 AM Zeus blane just wanted to see if you'd bite
 4/3/2008 11:55:07 AM Zeus blane i switching back to normal sign on now
 4/3/2008 10:52:01 AM bob blane BACK YET?????
 4/3/2008 10:52:28 AM blane bob no hold on will you
 4/3/2008 11:18:21 AM bob blane you back yet

yogibear19322121292544.xml

Date Time From To Message

4/3/2008 10:26:24 AM bob yogibear1953@hotmail.com back yet
 4/3/2008 10:26:35 AM yogibear1953@hotmail.com bob not yet
 4/3/2008 10:28:02 AM bob yogibear1953@hotmail.com have to go for a minute
 4/3/2008 10:28:16 AM yogibear1953@hotmail.com bob ok
 4/3/2008 10:52:01 AM bob blane BACK YET?????
 4/3/2008 10:52:28 AM blane bob no hold on will you
 4/3/2008 11:18:21 AM bob blane you back yet
 4/3/2008 11:59:06 AM blane bob hey im back you ther?
 4/3/2008 11:59:13 AM blane bob hey im back man
 4/3/2008 11:59:16 AM blane bob hey you on
 4/3/2008 11:59:28 AM bob blane yea i was on the can man
 4/3/2008 11:59:31 AM blane bob ok
 4/3/2008 11:59:44 AM bob blane everything good on your enc?
 4/3/2008 11:59:58 AM blane bob yea its ready im ready you?
 4/3/2008 12:00:16 PM bob blane Good, I tested out my speciaol black powder cake and man oh man
 4/3/2008 12:00:36 PM blane bob You didn't blow it all did you?
 4/3/2008 12:01:03 PM bob blane I aint that stupid Blaine
 4/3/2008 12:01:17 PM blane bob Hey, you said no names
 4/3/2008 12:02:12 PM bob blane Sorry, were even then. Listen I took a handful of the stuff, put in in that metal pipe with the ball berrings glued all over and went down to the dump at night.
 4/3/2008 12:03:10 PM bob blane Lit that bad mojo off and ran over the hill and dropped 'WHAM'. Took a quick look and what a hole and everything standing was shredded. What a ruswh.

Report of Examination

4/3/2008 12:03:34 PM blane bob So that's what they're talkin about on the news this morning
4/3/2008 12:03:51 PM bob blane News, what news? What u talking about?
4/3/2008 12:04:45 PM blane bob It was all over the news, some kind of explosion at the dump was reported. They're checking to see if it as like natural gass or something or some junk somebody threw away
4/3/2008 12:04:52 PM bob blane nuts
4/3/2008 12:05:29 PM blane bob they're going to figure this out man, that was a stupid play now they got the evidence
4/3/2008 12:05:52 PM bob blane they don't have jack, all they got is a hole and some busted stuff
4/3/2008 12:06:46 PM blane bob no, that was stupid. They got all this stuff to tell them what it was and who made it. I watch those shows on tv about them CSI dudes and they always figure it out
4/3/2008 12:07:50 PM blane bob whyd u have to do it so close to the city man, why not an out of state test
4/3/2008 12:24:54 PM bob blane cause mom wouldn't let me have the car last night and i couldn't drive it out of state even if i had it, no money for gas. So knock off that stupid stuff I did what I could. Least I was smart enough and I tested it out and those tv shows are just that and a bunch of stuff too.
4/3/2008 12:26:23 PM blane bob Man, I seen what they can do, they're gonna find us and grill us till we give up the whole thing
4/3/2008 12:26:29 PM bob blane That'
4/3/2008 12:27:57 PM bob blane That's garbage so knock it off, well pull this, nobody finds us and were rich. Aint you tired of being poor, working for sucker money. Only way they get on to us is if you open your mouth and blab it all over
4/3/2008 12:28:48 PM blane bob I don't rat, ut maybe we better not. Least not now.
4/3/2008 12:30:15 PM bob blane It goes as planned and you're gonna be there too. I didn't spend all this time and effort for you to chicken out at the last minute. If you're too yellow to work this with me ill get somebody else to pull it with. You just give me the guns and gear u got]
4/3/2008 12:30:55 PM blane bob I aint no more yellow than you. You think your so bad, just remember I can wip your tail anyway, did a year ago
4/3/2008 12:31:25 PM bob blane Then your'e in?
4/3/2008 12:31:48 PM blane bob You better believe it don't ever call me yellow again
4/3/2008 12:46:31 PM bob blane Ok, need you like we planned tomorrow night outside the warehouse. We go in while the guards are all at lunch, find the crates of ipods and get them out the door. Then we set the charges and get the stuff in the car and get out before the boom
4/3/2008 12:46:35 PM blane bob What about the guards
4/3/2008 12:46:44 PM blane bob guards
4/3/2008 12:48:15 PM bob blane If we stick to the schedule they're still at lunch in the front of the building and with the walls the blast will never get them but all the evidence will be blasted. Nothing to point them at us and they'll figure the stuff we stole was destroyed and probably won't even look for that stuff, just fugure gas blew or something
4/3/2008 12:48:23 PM blane bob Man I hop your right
4/3/2008 12:49:17 PM bob blane I am, and then we sell all those ipods for maybe 300 or 400 bucks each, couple of hundred of them, and figure the money with a 50 50 split. Lotta long green, keep you loaded a long time
4/3/2008 12:49:23 PM blane bob Sweet
4/3/2008 12:49:48 PM bob blane]So get a move on, I'll meet you there an hour before party time
4/3/2008 12:50:07 PM blane bob Done, im outta here
4/3/2008 12:50:24 PM bob blane Im gone too

Challenge Number: 401 - MSN Session Logs and Chat**Tool Information**

Type	Name	Publisher
<input checked="" type="radio"/> Commercial <input type="radio"/> Open Source	Internet Explorer	Microsoft
<input type="radio"/> Commercial <input type="radio"/> Open Source		
<input type="radio"/> Commercial <input type="radio"/> Open Source		
<input type="radio"/> Commercial <input type="radio"/> Open Source		
<input type="radio"/> Commercial <input type="radio"/> Open Source		

Notes

Found lots of sqm files

.SQM files are created by a number of Microsoft applications, most commonly Windows Live Messenger (previously known as MSN).

According to Microsoft, SQM files (standing for Software Quality Metrics) are used as part of their "Microsoft Customer Experience Program" and help improve their products by anonymously monitoring usage habits and reporting software errors/bugs.

According to microsoft these files do not contain any personal information, but they do show what functions the user is using. Unable to determine the format of these files

The other types of files seen is windows contact files which contain information for the user's contacts unable to determine whats in them, used a hex editor and notepad to look at them according to websites they are encrypted and only can be opened by the microsoft live service.

Looking at the files I guess the names of the contact files correspond to id's on the windows live servers?

DEF94150-805D-499B-84B0-B186ABDF7274.WindowsLiveContact

B00653A7-24DD-4E6F-82B4-78B4FAC433E1.WindowsLiveContact

1AC8CA47-1B2D-492C-9CF6-6F3737A5C2ED.WindowsLiveContact

To find the contacts one possible solution is to copy the contact files into an MSN Messenger folder for another user and see if they appear in the MSN Messenger window.

Type	Name	Publisher
<input type="radio"/> Commercial <input type="radio"/> Open Source		
<input type="radio"/> Commercial <input type="radio"/> Open Source		
<input type="radio"/> Commercial <input type="radio"/> Open Source		
<input type="radio"/> Commercial <input type="radio"/> Open Source		
<input type="radio"/> Commercial <input type="radio"/> Open Source		

Notes

I think the easiest way to get his contacts would be to attack the account directly

- guess the hotmail password?

- Hotmail site shows password can be reset by knowing location and secret question

This information could probably be gather by information on the user's computer

other than that, our user is as shown in the dialog below and the messenger contact list:

yogibear1953@hotmail.com

As for chat sessions

found xml files at the following path that contain text from chat sessions

D:\DC3\401_MSN_Session_Logs_and_Chat_Challenge2008

\401_MSN_Session_Logs_and_Chat_Challenge2008\MSN 1\MSN Messenger\My Received Files

\yogibear19534226628795\History

used internet explorer to view the xml files